In the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

1   1. (canceled).

1   2. (currently amended) The method of claim 31 [[1]], including ~~distributing symmetric~~

2   ~~encryption keys for use in a plurality of communication sessions using respective pluralities of~~

3   ~~exchanges, and~~ using said associated session key in response to another request to initiate a

4   communication session from a third station received by the first station ~~for first exchanges in the~~

5   ~~respective pluralities of exchanges for initiating communication sessions in the plurality of~~

6   ~~communication sessions initiated with the first station,~~ during said particular session key

7   initiation interval, and using other session keys from the set of ephemeral session keys after

8   expiry of said particular session key initiation interval.

1   3. (previously presented) The method of claim 2, including associating a unique set of

2   intermediate data keys with each session key.

1   4. (currently amended) The method of claim 31 [[1]], including:

2   providing a buffer at the first station;

3   storing the ~~an ephemeral~~ set of ephemeral session keys in the buffer; and ~~for respective~~

4   ~~session key lifetimes;~~

5   ~~———— associating respective session key initiation intervals with said session keys stored in said~~

6   ~~buffer;~~

7   ~~———— using session keys from the set of session keys from said buffer as session keys in~~

8   ~~response to requests received by said first station during said respective, associated session key~~

9   ~~initiation intervals;~~

10   removing session keys from said buffer upon expiry of [[the]] respective session key

11   lifetimes, said session key lifetimes being longer than the respective session key initiation

12   intervals.

1   5. (canceled).

1   6. (currently amended) The method of claim 4, wherein the session key lifetimes have respective

2   lengths longer or equal to a time required <u>for verification of mutual authentication using said first</u>

3   <u>and second sets of exchanges</u> <s>for the plurality of exchanges used to distribute the symmetric</s>

4   <s>encryption key for use in a communication session can be completed</s> in expected circumstances.

1   7. (currently amended) The method of claim 4, wherein the session key lifetimes have respective

2   lengths which are a multiple M times a time required <u>for verification of mutual authentication</u>

3   <u>using said first and second sets of exchanges</u> <s>for the plurality of exchanges used to distribute the</s>

4   <s>symmetric encryption key for use in a communication session can be completed</s> in expected

5   circumstances, where M is less than or equal to 10.

1   8. (canceled).

1   9. (currently amended) The apparatus of claim [[8]] <u>34</u>, including logic to <s>distribute symmetric</s>

2   <s>encryption keys for use in a plurality of communication sessions using respective pluralities of</s>

3   <s>exchanges, and to</s> use said <u>associated</u> session key <u>in response to another request to initiate a</u>

4   <u>communication session from a third station received by the first station</u> <s>for first exchanges in the</s>

5   <s>respective pluralities of exchanges for distributing the symmetric encryption keys in the plurality</s>

6   <s>of communication sessions initiated with the first station,</s> during said <u>particular</u> session key

7   initiation interval, and using other session keys <u>from the set of ephemeral session keys</u> after

8   expiry of said <u>particular</u> session key initiation interval.

1   10. (previously presented) The apparatus of claim 9, including logic to associate a unique set of

2   intermediate data keys with each session key.

1   11. (currently amended) The apparatus of claim [[8]] <u>34</u>, including

2   a buffer at the first station;

3   logic to store <u>the</u> <s>an ephemeral</s> set of <u>ephemeral</u> session keys in the buffer <s>for respective</s>

4   <s>session key lifetimes, to associate respective session key initiation intervals with particular</s>

5   ~~session keys in said set of session keys stored in said buffer, to use session keys from said buffer~~

6   ~~as session keys in response to requests received by said first station during said respective~~

7   ~~session key initiation intervals,~~ and to remove session keys in said set of <u>ephemeral</u> session keys

8   from said buffer after expiry of the respective session key lifetimes<u>, said session key lifetimes</u>

9   <u>being longer than the respective session key initiation intervals</u>.

1   12. (canceled).

1   13. (currently amended) The apparatus of claim 11, wherein the session key lifetimes have

2   respective lengths longer or equal to a time required <u>for verification of mutual authentication</u>

3   <u>using said first and second sets of exchanges</u> ~~for the plurality of exchanges used to distribute the~~

4   ~~secret encryption key for use in a communication session can be completed~~ in expected

5   circumstances~~, and including logic to remove said session keys in said set of session keys from~~

6   ~~said buffer after expiry of the session key lifetimes~~.

1   14. (currently amended) The apparatus of claim 11, wherein the session key lifetimes have

2   respective lengths which are a multiple M times a time required <u>for verification of mutual</u>

3   <u>authentication using said first and second sets of exchanges</u> ~~for the plurality of exchanges used to~~

4   ~~distribute the secret encryption key for use in a communication session can be completed~~ in

5   expected circumstances~~, and including logic to remove said session keys in said set of session~~

6   ~~keys from said buffer after expiry of the session key lifetimes~~.

1   15. (canceled).

1   16. (currently amended) The article of claim [[15]] <u>37</u>, wherein the instructions include logic to

2   ~~distribute secret encryption keys for use in a plurality of communication sessions using~~

3   ~~respective pluralities of exchanges, and to~~ use said <u>associated</u> session key <u>in response to another</u>

4   <u>request to initiate a communication session from a third station received by the first station</u> ~~for~~

5   ~~first exchanges in the respective pluralities of exchanges for assigning secret encryption keys in~~

6   ~~the plurality of communication sessions initiated with the first station,~~ during said <u>particular</u>

7   session key initiation interval, and using other session keys <u>from the set of ephemeral session</u>

8   <u>keys</u> after expiry of said <u>particular</u> session key initiation interval.

1   17. (previously presented) The article of claim 16, wherein the instructions include logic to

2   associate a unique set of ephemeral intermediate data keys with each session key.

1   18. (currently amended) The article of claim [[15]] <u>37, wherein</u>

2   the first station includes a buffer; and

3   the instructions include logic to store [[a]] <u>the</u> set of <u>ephemeral</u> session keys in the buffer

4   <s>for respective session key lifetimes, to associate respective session key initiation intervals with</s>

5   <s>particular session keys in said set of session keys stored in said buffer, to use session keys from</s>

6   <s>said buffer as session keys in response to requests received by said first station during said</s>

7   <s>respective session key initiation intervals,</s> and to remove session keys in said set of <u>ephemeral</u>

8   session keys from said buffer after expiry of the respective session key lifetimes<u>, said session key</u>

9   <u>lifetimes being longer than the respective session key initiation intervals</u>.

1   19. (canceled).

1   20. (currently amended) The article of claim 18, wherein the session key lifetimes have

2   respective lengths longer or equal to a time required <u>for verification of mutual authentication</u>

3   <u>using said first and second sets of exchanges</u> <s>for the plurality of exchanges used to distribute the</s>

4   <s>secret encryption key for use in a communication session can be completed</s> in expected

5   circumstances<s>, and the instructions include logic to remove said session keys in said set of</s>

6   <s>session keys from said buffer after expiry of the session key lifetimes</s>.

1   21. (currently amended) The article of claim 18, wherein the session key lifetimes have

2   respective lengths which are a multiple M times a time required <u>for verification of mutual</u>

3   <u>authentication using said first and second sets of exchanges</u> <s>for the plurality of exchanges used to</s>

4   <s>distribute the secret encryption key for use in a communication session can be completed</s> in

5   expected circumstances<s>, and the instructions include logic to remove said session keys in said set</s>

6   <s>of session keys from said buffer after expiry of the session key lifetimes</s>.

1   22-30. (canceled).

1   31. (new) A method for mutual authentication in communications between first and second

2   stations, comprising:

3   generating and storing a set of ephemeral session keys at the first station, ephemeral

4   session keys in the set being associated with respective session key initiation intervals, and being

5   discarded at a time later than expiration of the respective session key initiation intervals;

6   in response to a request to initiate a communication session received by the first station

7   during a particular session key initiation interval, selecting the associated session key;

8   sending a message carrying said associated session key to the second station, and

9   receiving a response from the second station including a digital identifier, the digital identifier

10   being information shared between the first station and the second station, or between the first

11   station and a user at the second station, the digital identifier being encrypted using said

12   associated session key to verify receipt of the session key by the second station and to identify

13   the second station or the user of the second station;

14   generating and storing, in the first station, a set of intermediate data keys, the set of

15   intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being

16   discarded at a time later than expiration of the particular session key initiation interval;

17   executing a first set of exchanges including one or more exchanges with the second

18   station, after verifying in said first station receipt of the session key by the second station by

19   decrypting the digital identifier using the associated session key at the first station and positively

20   matching the decrypted digital identifier against an existing entry in a stored list of authorized

21   users, the first set of exchanges including

22   sending a message to the second station carrying intermediate data key (i) from said

23   set of intermediate data keys encrypted using the associated session key for a

24   first exchange in first set of exchanges and using the intermediate data key (i-

25   1) for subsequent exchanges in the first set of exchanges,

26   receiving a response from the second station including a hashed version of

27   intermediate data key (i) encrypted using intermediate data key (i), decrypting

28   the hashed version of the intermediate data key (i), calculating a hashed

29   version of intermediate data key (i) at the first station, and matching the

30   calculated hashed version and the received hashed version of intermediate data

31   key (i) to verify receipt by the second station of intermediate data key (i);

32   executing a second set of exchanges for mutual authentication after verifying in said first

33   station receipt of the intermediate data key (n-1) by the second station, including

34   sending a first message carrying intermediate data key (n) encrypted using a hashed

35   version of a first shared secret,

36   receiving a response from the second station carrying a hashed version of intermediate

37   data key (n) encrypted using a hashed version of the first shared secret, and

38   decrypting the hashed version of the intermediate data key (n) , calculating a

39   hashed version of intermediate data key (n) at the first station, and matching

40   the calculated hashed version and the decrypted hashed version of intermediate

41   data key (n) to verify possession by the second station of the first shared

42   secret;

43   sending a second message carrying intermediate data key (n) encrypted using a hashed

44   version of a second shared secret; and

45   if the second station sends a response to the second message, carrying a hashed

46   version of intermediate data key (n) encrypted using a hashed version of the

47   second shared secret, after possession by the first station of the second shared

48   secret is verified at the second station, the verifying being accomplished at the

49   second station by decrypting the intermediate data key (n) from the second

50   message using the hashed version of the second shared secret, calculating a

51   hashed version of the intermediate data key (n), and matching the calculated

52   hashed version and the decrypted hashed version of intermediate data key (n)

53   to verify possession by the first station of the second shared secret, then

54   receiving the response from the second station, and decrypting the hashed version of

55   the intermediate data key (n) using the hashed version of the second shared

56   secret, calculating a hashed version of intermediate data key (n) at the first

57   station, and matching the calculated hashed version and the decrypted hashed

58   version of intermediate data key (n) at the first station to verify mutual

59   authentication of the first and second stations; and

60   if mutual authentication is verified at the first station, then sending a message indicating

61   successful authentication.

1   32. (new) The method of claim 31, wherein said message indicating successful authentication

2   carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of

3   said intermediate data keys (i).

1   33. (new) The method of claim 31, including using intermediate data key (n) as a symmetrical

2   key to encrypt data during post-authentication in communications between the first and second

3   stations in the communication session.

1   34.(new) A data processing apparatus, comprising:

2   a processor associated with a first station, a communication interface adapted for

3   connection to a communication medium, and memory storing instructions for execution by the

4   data processor, the instructions including

5   logic to receive a request via the communication interface for initiation of a

6   communication session between a first station and a second station;

7   logic to provide for mutual authentication in communications between the first station

8   and a second station, comprising:

9   generating and storing a set of ephemeral session keys at the first station, ephemeral

10   session keys in the set being associated with respective session key initiation intervals, and being

11   discarded at a time later than expiration of the respective session key initiation intervals;

12   in response to a request to initiate a communication session received by the first station

13   during a particular session key initiation interval, selecting the associated session key;

14   sending a message carrying said associated session key to the second station, and

15   receiving a response from the second station including a digital identifier, the digital identifier

16   being information shared between the first station and the second station, or between the first

17   station and a user at the second station, the digital identifier being encrypted using said

18   associated session key to verify receipt of the session key by the second station and to identify

19   the second station or the user of the second station;

20   generating and storing, in the first station, a set of intermediate data keys, the set of

21   intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being

22   discarded at a time later than expiration of the particular session key initiation interval;

23   executing a first set of exchanges including one or more exchanges with the second

24   station, after verifying in said first station receipt of the session key by the second station by

25   decrypting the digital identifier using the associated session key at the first station and positively

26   matching the decrypted digital identifier against an existing entry in a stored list of authorized

27   users, the first set of exchanges including

28   sending a message to the second station carrying intermediate data key (i) from said

29   set of intermediate data keys encrypted using the associated session key for a

30   first exchange in first set of exchanges and using the intermediate data key (i-

31   1) for subsequent exchanges in the first set of exchanges,

32   receiving a response from the second station including a hashed version of

33   intermediate data key (i) encrypted using intermediate data key (i), ~~and~~

34   decrypting the hashed version of the intermediate data key (i), calculating a

35   hashed version of intermediate data key (i) at the first station, and matching the

36   calculated hashed version and the received hashed version of intermediate data

37   key (i) to verify receipt by the second station of intermediate data key (i);

38   executing a second set of exchanges for mutual authentication after verifying in said first

39   station receipt of the intermediate data key (n-1) by the second station, including

40   sending a first message carrying intermediate data key (n) encrypted using a hashed

41   version of a first shared secret,

42   receiving a response from the second station carrying a hashed version of intermediate

43   data key (n) encrypted using a hashed version of the first shared secret, and

44   decrypting the hashed version of the intermediate data key (n) , calculating a

45   hashed version of intermediate data key (n) at the first station, and matching

46   the calculated hashed version and the decrypted hashed version of intermediate

47   data key (n) to verify possession by the second station of the first shared

48   secret;

49   sending a second message carrying intermediate data key (n) encrypted using a hashed

50   version of a second shared secret; and

51   if the second station sends a response to the second message, carrying a hashed

52   version of intermediate data key (n) encrypted using a hashed version of the

53   second shared secret, after possession by the first station of the second shared

54   secret is verified at the second station, the verifying being accomplished at the

55   second station by decrypting the intermediate data key (n) from the second

56   message using the hashed version of the second shared secret, calculating a

57   hashed version of the intermediate data key (n), and matching the calculated

58   hashed version and the decrypted hashed version of intermediate data key (n)

59   to verify possession by the first station of the second shared secret, then

60   receiving the response from the second station, and decrypting the hashed version of

61   the intermediate data key (n) using the hashed version of the second shared

62   secret, calculating a hashed version of intermediate data key (n) at the first

63   station, and matching the calculated hashed version and the decrypted hashed

64   version of intermediate data key (n) at the first station to verify mutual

65   authentication of the first and second stations; and

66   if mutual authentication is verified at the first station, then sending a message indicating

67   successful authentication.

1   35. (new) The apparatus of claim 34, wherein said message indicating successful authentication

2   carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of

3   said intermediate data keys (i).

1   36. (new) The apparatus of claim 34, including using intermediate data key (n) as a symmetrical

2   key to encrypt data during post-authentication communications between the first and second

3   stations in the communication session.

1

2   37. (new) An article, comprising:

3   machine readable data storage medium having computer program instructions stored

4   therein for establishing a communication session on a communication medium between a first

5   data processing station and a second data processing station having access to the communication

6   medium, said instructions comprising

7   logic to receive a request via the communication interface for initiation of a

8   communication session between a first station and a second station;

9   logic to provide for mutual authentication in communications between the first station

10   and a second station, comprising:

11   generating and storing a set of ephemeral session keys at the first station, ephemeral

12   session keys in the set being associated with respective session key initiation intervals, and being

13   discarded at a time later than expiration of the respective session key initiation intervals;

14   in response to a request to initiate a communication session received by the first station

15   during a particular session key initiation interval, selecting the associated session key;

16   sending a message carrying said associated session key to the second station, and

17   receiving a response from the second station including a digital identifier, the digital identifier

18   being information shared between the first station and the second station, or between the first

19   station and a user at the second station, the digital identifier being encrypted using said

20   associated session key to verify receipt of the session key by the second station and to identify

21   the second station or the user of the second station;

22   generating and storing, in the first station, a set of intermediate data keys, the set of

23   intermediate data keys including intermediate data key (i), for i = 1 to at least n, and being

24   discarded at a time later than expiration of the particular session key initiation interval;

25   executing a first set of exchanges including one or more exchanges with the second

26   station, after verifying in said first station receipt of the session key by the second station by

27   decrypting the digital identifier using the associated session key at the first station and positively

28   matching the decrypted digital identifier against an existing entry in a stored list of authorized

29   users, the first set of exchanges including

30   sending a message to the second station carrying intermediate data key (i) from said

31   set of intermediate data keys encrypted using the associated session key for a

32   first exchange in first set of exchanges and using the intermediate data key (i-

33   1) for subsequent exchanges in the first set of exchanges,

34   receiving a response from the second station including a hashed version of

35   intermediate data key (i) encrypted using intermediate data key (i), decrypting

36   the hashed version of the intermediate data key (i), calculating a hashed

37   version of intermediate data key (i) at the first station, and matching the

38   calculated hashed version and the received hashed version of intermediate data

39   key (i) to verify receipt by the second station of intermediate data key (i);

40   executing a second set of exchanges for mutual authentication after verifying in said first

41 station receipt of the intermediate data key (n-1) by the second station, including

42   sending a first message carrying intermediate data key (n) encrypted using a hashed

43   version of a first shared secret,

44   receiving a response from the second station carrying a hashed version of intermediate

45   data key (n) encrypted using a hashed version of the first shared secret, and

46   decrypting the hashed version of the intermediate data key (n), calculating a

47   hashed version of intermediate data key (n) at the first station, and matching

48   the calculated hashed version and the decrypted hashed version of intermediate

49   data key (n) to verify possession by the second station of the first shared

50   secret;

51   sending a second message carrying intermediate data key (n) encrypted using a hashed

52   version of a second shared secret; and

53   if the second station sends a response to the second message, carrying a hashed

54   version of intermediate data key (n) encrypted using a hashed version of the

55   second shared secret, after possession by the first station of the second shared

56   secret is verified at the second station, the verifying being accomplished at the

57   second station by decrypting the intermediate data key (n) from the second

58   message using the hashed version of the second shared secret, calculating a

59   hashed version of the intermediate data key (n), and matching the calculated

60   hashed version and the decrypted hashed version of intermediate data key (n)

61   to verify possession by the first station of the second shared secret, then

62   receiving the response from the second station, and decrypting the hashed version of

63   the intermediate data key (n) using the hashed version of the second shared

64   secret, calculating a hashed version of intermediate data key (n) at the first

65   station, and matching the calculated hashed version and the decrypted hashed

66   version of intermediate data key (n) at the first station to verify mutual

67   authentication of the first and second stations; and

68   if mutual authentication is verified at the first station, then sending a message indicating

69   successful authentication.

1   38. (new) The apparatus of claim 37, wherein said message indicating successful authentication

2   carries a signal encrypted using intermediate data key (n-1) or using another prearranged one of

3   said intermediate data keys (i).

1   39. (new) The apparatus of claim 37, including using intermediate data key (n) as a symmetrical

2   key to encrypt data during post-authentication communications between the first and second

3   stations in the communication session.

///